Submission from the Committee to Protect Journalists
to the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression in response to the
Call for Submissions: The Surveillance Industry and Human Rights

In response to the request by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the Committee to Protect Journalists submits the following information on the surveillance industry and human rights, based on our experience protecting journalists and promoting press freedom globally. CPJ is an independent, nonprofit, nongovernmental organization, established in 1981, based in New York, that accepts no governmental or intergovernmental funding and defends the rights of journalists to report the news safely and without fear of reprisal.

Through our network of correspondents around the world, CPJ regularly hears from journalists in the field that their work—and safety—are undermined by government attempts to intercept and spy on their communications. The freewheeling trade in surveillance and monitoring technology, which allows governments with worrying press freedom records to purchase advanced tools on the open market, puts journalists and their sources' lives in danger, contributes to an atmosphere of fear, and chills critical reporting. As CPJ noted in 2015, the proliferation of surveillance is creating pressure for journalists to act more and more like spies themselves, a dynamic that is toxic for press freedom: "when journalists must compete with spies and surveillance, even when they win, society loses."[1] The situation has only worsened in the intervening years.

Our research has shown:
-There appear to be few effective barriers preventing oppressive governments, with demonstrated histories of surveilling and curtailing the free press, from acquiring sophisticated surveillance technology on the open market
-This technology is increasingly sophisticated and undetectable, with tools that reportedly can allow a government to surreptitiously take control of a journalist's device without the user taking any action (such as clicking on a link)[2]
- In many cases the only reason we do know about technologies being used against journalists is because journalists have investigated and reported on them

[1] https://cpj.org/2015/04/attacks-on-the-press-surveillance-forces-journalists-to-think-act-like-spies.php
[2] https://motherboard.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo

- There appear to be few, if any, frameworks for assessing the press freedom or broader human rights impact of surveillance technologies in advance of their sale to states that are known to target journalists. There is no indication that firms involved in the sale of surveillance technologies to governments or state actors are abiding by the UN Guiding Principles on Business and Human Rights or the UN "Protect, Respect, Remedy" framework
-The result is an increasingly hostile environment for reporters and their sources. In some cases, states appear to be surveilling journalists, and their colleagues, immediately before or after their murders. Journalists are increasingly worried that sources will be compromised, and potentially harmed, by states deploying sophisticated surveillance measures and determined to quiet critical coverage.

CPJ has been tracking these trends as they spread across the globe. For example, over the past year, CPJ and others have documented how Saudi Arabia likely deployed Israeli-made, American-owned surveillance technology to monitor close associates of *Washington Post* journalist Jamal Khashoggi immediately before his murder.[3] One of those associates, Omar Abdulaziz, has told CPJ that he believes the information Saudi Arabia gleaned from that surveillance motivated the government's decision to murder Khashoggi. The surveillance vendor that supplied the Saudi security services with intrusion malware, the Israeli firm NSO Group Technologies, and its American owners at the time, Francisco Partners, both claim to have acted within the laws of their respective jurisdictions.[4]

A similar pattern has unfolded recently in Mexico. In late 2018, digital rights groups revealed that two journalists at the Mexican outlet *RioDoce* were targeted by the same sophisticated Israeli spyware likely deployed against Khashoggi's associates.[5] These journalists were colleagues of the murdered Mexican reporter Javier Valdez, the winner of CPJ's 2011 International Press Freedom Award. At least eight Mexican reporters have likely been targeted by the government with the same spyware—which the Mexican government continued to deploy against journalists, even after the behavior was exposed and highlighted by journalists, digital rights organizations, and CPJ.

As Surveillance Technology Spreads, It Can Undermine Press Freedom

Surveillance is inherently difficult to trace, and given the opaque nature of the trade—and the patchwork of rules regulating it—documenting concrete cases involving journalists can be a challenge. Still, the public record is disturbing: a steady stream of surveillance know-how and tools is flowing into the hands of governments and security agencies that CPJ has identified as press freedom abusers. In some of the cases we have documented, that technology was

[3] https://cpj.org/blog/2018/10/how-the-saudis-may-have-spied-on-jamal-khashoggi.php
[4] https://www.washingtonpost.com/opinions/2018/12/12/washington-must-wake-up-abuse-software-that-kills/?utm_term=.813937751c0f
[5] https://www.nytimes.com/es/2018/11/27/javier-valdez-riodoce-pegasus/

developed by firms in the OSCE and OSCE partner countries, such as the United States, Israel, the United Kingdom, and EU member countries, and deployed against reporters doing critical journalism.

In some cases, researchers have been able to detect discrete incidents of surveillance, and identify the firms implicated. In late 2017, for example, Citizen Lab documented a sustained effort to hack and surveil the Ethiopian Oromia Media Network and its head, Ethiopian reporter Jawar Mohammed, using intrusion software sold by the Israeli firm Cyberbit. CPJ reported on how those attempted hacks fit into a wider crackdown on journalists in Ethiopia since the country's state of emergency in late 2016.[6]

In many cases, a clear pattern of surveillance emerges, but not all of the pieces—the agency involved in surveillance, the names of victims, the surveillance vendor, and the immediate consequences—have been exposed.

In the United Arab Emirates, for example, the American firm CyberPoint worked with the government and the UAE firm DarkMatter to build surveillance infrastructure that targeted an unknown number of journalists; at least three American reporters and one British reporter were targeted, according to a 2019 Reuters report.[7] CPJ has independently documented a worrying tendency by the government of the UAE to conflate critical journalism with criminal activity, and to disappear journalists without due process.[8] The country has a long history of using spyware against its citizens. In 2009, CPJ Advocacy Director Courtney Radsch was working as a journalist in Dubai and received an update notification from the state-owned telecom Etisalat for her Blackberry device, along with 145,000 other users, that was later confirmed by device maker RIM to contain spyware that would enable unauthorized access to private information.[9]

This is a pattern we have observed globally: the opaque acquisition and deployment of surveillance technology in countries with troubling press freedom practices.

In Egypt, CPJ has reported on a disturbing campaign of surveillance and hacking targeting journalists, potentially facilitated by foreign firms, including the American firm Symantec.[10] Other digital rights organizations, including Privacy International, Citizen Lab, and the International Center for Human Rights have documented how the Egyptian government went on a global buying spree going back at least a decade, acquiring surveillance equipment from companies around the world. For example, at least five French firms sold a range of surveillance capabilities to Egypt; the U.S. firms Narus and Sandvine appear to have sold Egypt deep packet

[6] https://cpj.org/blog/2018/01/why-release-of-two-journalists-in-ethiopia-does-no.php
[7] https://cpj.org/2019/01/cpj-concerned-by-report-that-uae-project-raven-sur.php
[8] https://cpj.org/2016/02/jordanian-journalist-held-incommunicado-in-abu-dha.php
[9] http://news.bbc.co.uk/2/hi/8161190.stm
[10] https://cpj.org/blog/2017/06/how-surveillance-trolls-and-fear-of-arrest-is-affe.php

inspection capabilities; and the Italian firm Hacking Team has sold intrusion malware to Egypt.[11] Over the past several years, CPJ has documented a brutal crackdown on journalists in Egypt, which has become the global leader in imprisoning journalists on trumped up "fake-news" charges.[12] It has been among the top three countries jailing journalists for three years in a row.[13]

In Uganda, CPJ reported in 2018 how President Yoweri Museveni personally threatened reporters who reported critically on his policies.[14] Over the last five years, the government of Uganda has acquired intrusion malware capabilities furnished by the British firm Gamma Group and its FinFisher technology, which can remotely monitor computers, smartphones, and other equipment in real-time. According to Privacy International, Ugandan security forces used intercepted communications to intimidate journalists working on sensitive stories. The Ugandan government was also in talks with a number of firms to build a centralized mass surveillance system, including the Chinese firms Huawei and ZTE, the Israeli firms NICE and Verint, and the Italian firm Hacking Team.[15]

In 2018, CPJ issued a report on the press freedom situation in Pakistan, highlighting the singular role the country's military plays in ensuring that many journalists who do critical work are "attacked, threatened, or arrested."[16] Pakistan has reportedly deployed a full spectrum of surveillance capacities—including intercepting phone calls and surveilling emails—furnished by an expansive group of foreign companies.[17] This surveillance can potentially have a devastating impact on journalists who write critically about the state. In one specific instance, CPJ documented how Pakistani journalist Ahmed Noorani, who investigates the military, was assaulted in a highly coordinated attack while en route to an appointment he had arranged on a rarely-used open phone line.[18] According to Privacy International, a number of foreign firms have been involved in building network surveillance in Pakistan, including the German firms Trovicor and Utimaco and the Chinese firm Huawei.[19]

In Colombia, CPJ has documented a long history of state surveillance of a number of prominent journalists. During President Álvaro Uribe's tenure from 2002 to 2010, a state intelligence agency surveilled prominent journalists, including Alejandro Santos, Daniel Coronell, Julio Sánchez Cristo, Darío Arizmendi, Ramiro Bejarano, Claudia Julieta Duque, and Hollman

[11] https://privacyinternational.org/state-privacy/1001/state-privacy-egypt
[12] https://cpj.org/reports/2018/12/journalists-jailed-imprisoned-turkey-china-egypt-saudi-arabia.php
[13] https://cpj.org/imprisoned
[14] https://cpj.org/2018/09/ugandan-police-arrest-at-least-8-journalists-cover.php
[15] https://privacyinternational.org/state-privacy/1013/state-privacy-uganda
[16] https://cpj.org/reports/2018/09/acts-of-intimidation-pakistan-journalists-fear-censorship-violence-military.php
[17] https://privacyinternational.org/report/1635/tipping-scales-security-and-surveillance-pakistan
[18] https://cpj.org/2017/10/pakistani-journalist-attacked-in-islamabad-three-a.php
[19] https://privacyinternational.org/report/1635/tipping-scales-security-and-surveillance-pakistan

Morris.[20] Even after the intelligence agency was dissolved and Colombia adopted some modest reforms, CPJ documented suspected state surveillance of journalists Claudia Morales and Vicky Dávila in 2016.[21] In 2016, CPJ documented how anonymous emails threatened reporters that Colombian police had private photos of their family members. Over the last 15 years, a number of foreign technology firms built out the Colombian security service's surveillance capabilities, including intrusion malware supplied by Hacking Team in 2014 and monitoring systems supplied by Verint and NICE Systems in 2005, according to Privacy International.[22]

CPJ is also concerned about the impact of surveillance on press freedom in Morocco. In recent interviews with five independent Moroccan journalists, CPJ documented a devastating chilling effect: journalists report constant fear of being tracked, having to constantly replace devices, and seeing emails sent from their accounts that they never sent themselves.[23] This dynamic has forced reporters to self-censor and some even to flee the country. According to Privacy International, the Morocco intelligence agencies have acquired advanced intrusion malware from foreign suppliers, including Hacking Team, Gamma Group, as well as monitoring capabilities from the British firm BAE.[24]

In China, the state appears simultaneously committed to cementing a surveillance regime at home while exporting those capabilities abroad. Journalists in China tell CPJ that they assume their digital communications are constantly under state surveillance.[25] According to the Foreign Correspondents Club 2018 annual survey, 91 percent of journalists surveyed worried about the security of their phones and 66 percent worried about surveillance inside their own homes or offices. In 2018, CPJ ranked China as the second most prolific jailer of journalists in the world.[26] China is also emerging as a major exporter of both surveillance technology and cyber-governance models. In 2018, Freedom House warned that China was in the midst of remaking "the world in its techno-dystopian image,"[27]citing a number of recent examples, including Chinese-modeled cyber security legislation in Vietnam and Chinese supplied facial recognition technology in Zimbabwe.

When press-abusing governments are subject to some degree of transparency, the scope of their surveillance practices can become clearer—as does the threat posed to reporters. That's what happened in the wake of the Arab Spring, when governments fell and national security archives were examined by activists and the media. During the 2011 revolution in Egypt, for example,

[20] https://cpj.org/2015/05/officials-sentenced-in-colombia-for-spying-on-jour.php
[21] https://cpj.org/blog/2016/02/claims-police-spied-on-two-journalists-revive-surv.php and https://cpj.org/blog/2016/02/are-intelligence-sector-reforms-enough-to-protect-.php
[22] https://privacyinternational.org/state-privacy/58/state-privacy-colombia
[23] Based on CPJ interviews conducted in 2018 and 2019
[24] https://www.privacyinternational.org/state-privacy/1007/state-privacy-morocco
[25] https://cpj.org/blog/2018/03/censorship-surveillance-and-harassment-china-crack.php
[26] https://cpj.org/reports/2018/12/journalists-jailed-imprisoned-turkey-china-egypt-saudi-arabia.php
[27] https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism

activists gained access to security archives housing surveillance records. Sherif Mansour, CPJ's Middle East Program Coordinator—then working at Freedom House—obtained copies of his own emails and print-outs of his Skype calls that the government had surveilled using FinFisher software sold by the British firm Gamma Group.[28] In Libya, after the fall of Gaddafi in 2012, the *Wall Street Journal* gained access to a government building where Libyan security agents deployed the Eagle System, a surveillance tool that allowed the government to snoop on emails and internet traffic, supplied by the French firm Amesys. The *Journal* observed dozens of surveillance dossiers, including files on Libyans who operated websites critical of the Gaddafi government. The Libyan government had also put Heba Morayef, a Human Rights Watch staffer, under surveillance and had copies of her correspondence on file.[29]

Surveillance technology can be incredibly dangerous in the hands of states determined to squash dissent and silence critical journalism. Yet, companies that manufacture and sell these capabilities have been able to sell them across borders and they continue to supply press-abusing regimes with advanced surveillance capacities, even in cases where that specific technology has been linked to abuse. In Mexico, for example, starting in 2015 the government repeatedly deployed the Israeli-made, American-owned Pegasus surveillance exploit against journalists. Civil society groups, including CPJ, documented the attacks. However, Mexican journalists continued to be targeted well into 2017.[30] There is no indication that NSO Group ran into any legal problems with export licenses in Israel or the United States. And in Mexico, civil society groups are still unable to identify which exact members of the Mexican security forces deployed Pegasus against journalists, how NSO Group responded to complaints about the misuse of its product, and whether any new safeguards have been established to prevent future abuse. NSO Group reportedly devised "Business Ethics Framework" guidelines to decide which governments can purchase Pegasus, with the assistance of Beacon Strategies and Francisco Partners, yet this framework is opaque and it is unclear whether it includes consideration of press freedom or human rights, and the companies involved have not responded to CPJ's requests for additional information.

In another example, the American firm CyberPoint obtained a special export license from the U.S. State Department to provide cyber training for the United Arab Emirates.[31] At the same time, CPJ was issuing warnings about the UAE's "categorical intolerance for dissent."[32] In 2019, Reuters revealed that CyberPoint worked with the UAE government to surveil American journalists; the details of this apparent press freedom violation are still unclear, and there has

[28] https://www.washingtontimes.com/news/2011/apr/25/british-firm-offered-spy-software-to-egypt/
[29] https://goodtimesweb.org/surveillance/wsj-libya-spies-firms-aug-30-2011.html
[30] https://www.nytimes.com/2018/11/27/world/americas/mexico-spyware-journalist.html
[31] https://www.washingtonpost.com/world/national-security/as-cyberwarfare-heats-up-allies-turn-to-us-companies-for-expertise/2012/11/22/a14f764c-192c-11e2-bd10-5ff056538b7c_story.html?utm_term=.7b4454b07f14
[32] https://cpj.org/2011/06/uae-intent-on-punishing-online-dissent.php

been no indication that either the UAE or CyberPoint will disclose the extent of the damage, or reform their practices.

Towards More Transparency and a Human Rights Framework

CPJ has joined with partner organizations in calls to strengthen the export control regime for surveillance technology. At the European Union level, CPJ backed a proposal that would force member states to deny export license to firms if they sell technology that "is likely to lead to serious human rights violations."[33] It would also require that authorities "assess an exports' impact on the right to privacy, the right to data protection, freedom of speech, and freedom of assembly and association." This proposal would also add significant transparency mechanisms, requiring member states to publish licensing data regarding approved and denied exports. Such transparency reporting should be a minimum requirement, yet it has faced opposition from some member states.

The UN has repeatedly recognized that the surveillance of journalists can undermine press freedom and violate rights to privacy and freedom of expression. A 2014 UN General Assembly Resolution on the Safety of Journalists and the Issue of Impunity pointed out the "particular vulnerability of journalists to becoming targets of unlawful or arbitrary surveillance or interception of communications in violation of their rights to privacy and to freedom of expression." And in 2013, UNESCO member states recognized the importance of source protection to the exercise of a free press.[34]

The surveillance industry is a global phenomenon, traversing national boundaries and markets; it is therefore appropriate for the United Nations to take an interest in its inner workings. Recent history demonstrates that transparency and oversight over the private surveillance trade are necessary for the safety of journalists and the promotion of press freedom globally. Human rights considerations must be taken into account in the export of these dangerous technologies as well, especially the press freedom records of end-users. It is also clear that the obligation to ensure this dangerous technology stays out of the hands of those who would target journalists is broadly shared, by business, civil society, governments, and international organizations, and we would welcome UN leadership on this crucial issue.

[33] https://cpj.org/blog/2018/01/cpj-joins-call-for-eu-to-stop-surveillance-softwar.php
[34] https://en.unesco.org/system/files/reviewreportunplan_of_action_on_safety_of_journalist_fin.pdf